PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04K 1/00 | A1

(11) International Publication Number: **WO 00/19652**

(43) International Publication Date: 6 April 2000 (06.04.00)

(21) International Application Number: PCT/US99/22710

(22) International Filing Date: 1 October 1999 (01.10.99)

(30) Priority Data:

60/102,633	1 October 1998 (01.10.98)	US
60/131,833	29 April 1999 (29.04.99)	US

(71)(72) Applicants and Inventors: POOVENDRAN, Raadhakrishnan [LK/US]; P.O. Box 474, Greenbelt, MD 20768 (US). CORSON, Mathew, Scott [US/US]; 10122 Ashwood Drive, Kensington, MD 20895 (US). BARAS, John, S. [US/US]; 10912 Burbank Drive, Potomac, MD 20854 (US).

(74) Agents: SOKOHL, Robert, E. et al.; Sterne, Kessler, Goldstein & Fox P.L.L.C., Suite 600, 1100 New York Avenue, N.W., Washington, DC 20005–3934 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: DISTRIBUTED SHARED KEY GENERATION AND MANAGEMENT USING FRACTIONAL KEYS

(57) Abstract

A class of distributed key generation (130) and recovery (125) approaches is presented, suitable for group communication systems where the group membership must be tightly controlled. The proposed key generation (130) approach allows entities which may have only partial trust in each other to jointly generate (130) a shared key without the aid of an external third party. The group collectively generates (130) and maintains a dynamic group binding parameter (110), and the shared key is generated (110) using a pseudorandom function (110) using this parameter as a seed. The methods employ distributed algorithms based on fractional keys (FK) (515). The proposed methods allow the members to automatically update the keys in a periodic manner without any assistance from an external third party, and to do so using verifiable secret sharing techniques. The key retrieval method (125) does not require the keys to be stored in an external retrieval center. Note that many Internet–based applications may have these requirements.